a. an authentication step of creating a collection of records about a plurality of individuals by entering into a data storage medium a collection of any or a combination of any of the following:

   i. personal information about an individual,

   ii. an indicator of the reliability of the identification of the individual who is the subject of a record,

   iii. whether the authentication mode is universal or whether such individual must authenticate to the server computer in order to sign electronic data using the server computer, and

   iv. the authentication credential or plurality of authentication credentials that such individual must present to the server in order to sign;

b. an access control step of

   i. receiving a request to sign and, unless the authentication mode is universal, an authentication credential or a plurality of authentication credentials from a requestor, and

   ii. comparing the authentication credential or credentials to the information contained in the collection of records to determine if the requestor is an individual who is authorized to sign electronic data using the server;

c. a presentation step of providing to the server the electronic data for signature by the server computer;

d. a transaction identifier step of generating at the server a globally unique transaction identifier for the electronic data that a requestor intends to sign;

e. a signature step whereby the server signs the electronic data using an encryption device located at the server;

f. a recording step in which the server generates and stores in a data storage medium a record of a signature transaction;

g. a verification step whereby

i. an inquiring party seeking to verify the fact and validity of a signature of electronic data transmits to a server electronic data that is believed to have been previously signed by the server;

ii. the server determines if a record or a plurality of records corresponding to the transmitted signed electronic data exists in the data storage medium of such records;

iii. the server retrieves a record or plurality of records corresponding to the electronic data which is presented for verification;

iv. the server determines by an encryption device located at the server whether the electronic data was signed at the server, the identity of the signer or plurality of signers of the electronic data and if the electronic data has been modified since a signature was generated; and

v. the server reports to the inquiring party the results of the determination conducted in the previous step.

whereby electronic data is signed and verified at a server without the need for a unique client-side digital certificate of the client or signature tablet connected to the client user's computing device.

57. The method of claim 56 wherein the authority of an individual to sign on behalf of an entity or other person, and any dollar or legal limit imposed is included in an authentication credential of such individual.

58. The method of claim 56 wherein the electronic data to be signed at the server computer is generated at the server computer from information collected from a requestor and a document template which resides on the server, and which information and template are

merged at the server computer into an electronic record, message, communication or electronic data file and signed upon a command or plurality of commands of the requestor.

59. The method of claim 56 wherein a globally unique transaction identifier of a signature transaction includes the date and time of signature as determined by the server computer based upon the local time zone in which the server computer is located or the Greenwich Mean Time equivalent thereof.

60. The method of claim 56 wherein a transaction record of signed electronic data that is entered into a data store contained in the collection of signature records consists of:

    a. a globally unique transaction identifier,

    b. a date and time of signing,

    c. an identifier of a signer,

    d. an identifier of the electronic data that was signed,

    e. a message digest value of the electronic data or encrypted signature value, and

    f. an assurance level of identification of the signer.

61. The method of claim 56 wherein the server computer simultaneously accepts authentication credentials from a plurality of requestors for access to the encryption signature device of the server which credentials consist of any or a plurality of any of the following: a biometric identifier, a username and password, a passphrase, a personal identification number, a digital certificate for identity purposes, a smart card, a key token, a secret code, a credit card transaction authorization approval code, or a combination of any of them but excluding authentication based on local domain security services on a client–server network with public-key or Kerberos authentication and key establishment.

62. The method of claim 61 wherein authentication is determined on the basis of a digital certificate from a collection of types and classes of digital certificates issued by a

plurality of certification authorities for the purpose of authenticating the subjects named therein, comprising:

(a) An investigation step into the reliability of a plurality of identification procedures that are used to register individuals and issue to them digital certificates from a plurality of certification authorities, in light of the authentication needs of a party or plurality of parties intending to rely upon electronic signatures to be generated at the server computer;

(b) A selection step from among the plurality of such certification authorities of a plurality of types and classes of digital certificates that are considered to be acceptable for authenticating the subjects named in the certificates in order to sign electronically at the server computer;

(c) An implementation step whereby the server computer is instructed to accept as authenticated for signature purposes a signer named as a subject in a type and class of digital certificate that has been selected as acceptable;

(d) An access control step to deny a requestor access to an encryption device of the server computer unless a digital certificate of a type and class that has been selected as acceptable for authentication is furnished by the requestor,

whereby documents are signed and verified in accordance with authentications contained in various types and classes of digital certificates issued by different certification authorities without a need to cross-certify the certification authorities of the certificates, to accord due diligence regarding the reliability of registration procedures employed in connection with the issuance of identity digital certificates, and to reduce the costs and overhead of electronic signatures associated with digital certificates.

63. The method of claim 56 wherein the server's encryption device consists of a unique encryption key, generated from a symmetric cipher using a globally unique transaction

identifier of an electronic data transaction as the character input of a password for generation of the key,

whereby each document to be signed is encrypted with a unique symmetric key, and whereby a cryptotransformation of a document involving the application of such key constitutes a signer's signature.

64. The method of claim 56 wherein the message digest of the electronic data which is signed is used as a globally unique transaction identifier.

C1 cont

65. The method of claim 56 wherein the electronic data consists of a document to be signed that includes formatting tags or codes,

whereby the document can be read by applications that employ such tags or codes after completion and signature.

66. The method of claim 58 wherein the document to be signed includes server-supplied text or graphical information that is displayed to the client user but cannot be modified or deleted by the user,

whereby signature by the client user indicates acceptance and agreement to the supplied text and graphical information as part of the signed document information.

67. The method of claim 56 wherein a user signs by any of a plurality of the following:

a. speaking a voice command,
b. moving a computer mouse,
c. clicking a computer mouse,
d. pressing a key on a keyboard or keypad,
e. pressing a stylus on a pad, or
f. pressing a stylus or finger on a screen.

68. The method of claim 56 wherein the signed electronic data consists of an envelope for the transmission and routing of logically associated files, each of which is independently signed using an encryption means.

69. The method of claim 56 wherein the signer is an electronic process or agent not under the immediate control of a human being.

70. A method of electronically signing and verifying the signature of an electronic transaction record, document, filing, message, binary file or other digital information (hereinafter collectively referred to as "a document" or "the document"), comprising:

a. under control of a client system,

1. sending a client user identifier to a server system;

2. presenting a document to be signed by the server system; and

3. displaying a choice of actions to be taken by the user to confirm an intent to sign the document using an encryption device of the server as an act of signature by the user of the client system; and

b. under control of the server system,

1. controlling access by clients to the server on the basis of based client identifiers;

2. electronically signing the document using an encryption device stored on the server system upon command by a client user; and

3. with an encryption device stored on the server system, having the server verify to a relying party the unchanged message contents of an

electronically document previously signed using the server and the identity of the client user on whose behalf it was signed,

whereby the document is both electronically signed on behalf of the client user and verified by a relying party using the server computer, without any client-side encryption keys distributed to a signing or relying party, or a need for interoperability of keys or certification authorities.

71. The method of claim 70 wherein the server computer used for signing generates a unique identifier for the document to be signed that includes a sequence of a combination of one or more computer network location identifiers, together with a reference to the client side identifier of the person or entity on whose behalf signing occurs, and the current date and time as reported by the server's clock.

72. The method of claim 71 wherein the server system:

1. stores each unique document identifier in a database at or accessible to the server as a record of each signature transaction;

2. at the request of a client side user or a relying party, queries one or more of a collection of unique document identifiers at the server system; and

3. retrieves and displays, on the basis of each particular unique document identifier supplied, related records to the client side user or relying party, containing information about a signed document, including information about the person or entity on whose behalf a signature was made.

73. The method of claim 70 wherein the method of the server system to authenticate a user includes any or a plurality of any of the following

a. an approval code generated by a credit card payment system and transmitted to the server computer prior to signing on behalf of a credit card user,
b. a passphrase,